PTO/SB/21 (08-08)
Approved for use through 09/30/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paper Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM (to be used for all correspondence after initial filing)			
		Application Number	10/691,216
		Filing Date	Oct 22, 2003
		First Named Inventor	Han, Richard A.
		Art Unit	2131
		Examiner Name	Moorthy, Aravind K.
Total Number of Pages in This Submission		Attorney Docket Number	500.0344 (10806.00)

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
- ☐ Fee Attached
- ☐ Amendment / Reply
- ☐ After Final
- ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
- ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ Landscape Table on CD
- ☐ After Allowance communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Priest & Goldstein, PLLC		
Signature	Peter H. Priest		
Printed name	Peter H. Priest		
Date	February 11, 2009	Reg. No.	30210

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature	Marianna Tortorelli		
Typed or printed name	Marianna Tortorelli	Date	February 11, 2009

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

500.0344
10806.00

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Han et al.

Serial No.: 10/691,216

Filed: October 22, 2003

For: CONTROLLED ACCESS TO SOFTWARE APPLICATIONS AND/OR DATA

Group: 2131

Examiner: Moorthy, Aravind K.

Durham, North Carolina
February 11, 2009

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response

Sir:

In response to the Notification of Non-Compliant Appeal Brief mailed January 15, 2009, enclosed is a revised Appeal Brief.

Respectfully submitted,

Peter H. Priest
Reg. No. 30,210
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, NC 27713-7736
(919) 806-1600

500.0344 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Han et al.
For	:	Controlled Access to Software Applications And/Or Data
Serial No.	:	10/691,216
Filed	:	10/22/2003
Group	:	2131
Examiner	:	Moorthy, Aravind K.

Durham, North Carolina
December 15, 2008

MAIL STOP APPEAL BRIEF – PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF

Sir:

1. The Real Party In Interest

The real party in interest is the assignee, NCR Corporation.

2. Related Appeals and Interferences

None.

3. Status of the Claims

This is an appeal from the July 15, 2008 final rejection ("the final rejection") of claims 1-10 and 12-20, all of the pending claims. Claims 1-10 and 12-20 were rejected under 35 U.S.C.

§ 102(e) based on Hauck U.S. Patent No. 7,249,262 (Hauck). Claim 11 has been previously canceled.

4. Status of Amendments

The claims stand as last amended on April 28, 2008. No Amendment After Final has been filed.

5. Summary of Claimed Subject Matter

The present invention addresses techniques for identifying devices authorized for access to software or data, and for providing such access only to authorized devices.

Claim 1

In one aspect, the invention of claim 1 addresses a system for a licensee to control access to or distribution of software and/or data among a plurality of client nodes. The system comprises means for storing software and/or data that is to be made available to predetermined licensed client nodes, as described at p. 2, lines 4-6, for example. Each client node of the plurality of client nodes is a data processing device for which access to specified software or data may be allowed if licensed, and the system comprises means for storing a list of identifiers for licensed client nodes, with each identifier uniquely identifying one of the predetermined nodes, the presence of each identifier on the list authorizing the predetermined client node associated with the identifier to be allowed access to the software and/or data, as illustrated at Fig. 1, steps 101 and 102, and Fig. 3, server 301, database 303, for example, and discussed at specification, p. 4, line 22-p. 5, line 5; and p. 6, line 11-p. 7, line 2, for example. Claim 1 further addresses a client application at each client node, the client application performing authentication taking place at the client node, authentication being accomplished by comparing the client identifier for the node against the list and allowing or rejecting access to the software and/or data by the client

node at which the client application resides based on evaluation by the client application at the client node as to whether the identifier of the client node appears in the list, as illustrated at Fig. 3, CD 310, and discussed at specification, p. 5, lines 11-15 and p. 7, lines 12-19, for example.

Claim 9

In another aspect, the invention of claim 9 addresses a method for a licensee to control access to or distribution of software and/or data among a plurality of client nodes. The method comprises storing in association with the software and/or data, a list of unique identifiers for licensed client nodes, each of which uniquely identifies one of the nodes authorized to be allowed access to the software and/or data, as illustrated at Fig. 1, step 103 and discussed at specification, p. 4, line 22-p. 5, line 6, for example. Claim 9 further addresses identifying at each node whether a unique identifier for a particular node is included on the list, and controlling the operation of each node so that the list is examined at each node and the unique identifier is compared against the list, and loading, installation, or use of the software and/or data is allowed or rejected based on the comparison at the client node of the unique identifier against the list, as illustrated at Fig. 2, steps 202-206, and discussed at specification, p. 5, lines 20-27, for example.

Claim 10

In another aspect, the invention of claim 10 addresses a program storage device, readable by a machine, having encoded thereon instructions executable by the machine for executing a license management program to establish a unique identifier associated with the machine executing the instructions, reading a list of unique identifiers associated with specified software and/or data, each unique identifier being uniquely associated with one of a plurality of machines and establishing its associated machine as licensed for the specified software and/or data, and controlling the operation of a client node comprising the machine executing the instructions so as

to allow or reject access by the machine to the software and/or data based on a comparison taking place at the client node of the unique identifier for the client node against the list of unique identifiers, as illustrated at Fig. 3, floppy disc 308, CD 310, and discussed at specification, p. 6, line 11-p. 7, line 19, for example.

Claim 13

In another aspect, the invention of claim 13 addresses data processing device serving as a client node comprising means for reading a list of unique identifiers associated with software and/or data, each unique identifier being uniquely associated with one of a plurality of client nodes or terminals licensed to use the software and/or data and means for controlling the operation of the data processing device so that the data processing device examines its own unique identifier and the list of unique identifiers and allows or rejects loading, installation, or use of the software and/or data based on a comparison taking place at the data processing device of its own unique identifier against the list of unique identifiers, as illustrated at Fig. 3, client node 302, and discussed at specification, p. 6, line 11-p. 7, line 19, for example.

Claim 16

In another aspect, the invention of claim 16 addresses a self-service terminal comprising means for reading a list of unique identifiers associated with software and/or data, each unique identifier being uniquely associated with one of a plurality of self-service terminals licensed to use the associated software and/or data and means for controlling the operation of the self-service terminal so that the self-service terminal examines a unique identifier associated with the self-service terminal and the list of unique identifiers and allows or rejects loading, installation, or use of the software and/or data based on a comparison taking place at the self-service terminal of the unique identifier of the self-service terminal against the list of unique identifiers, as

illustrated at Fig. 3, client node 302, and discussed at specification, p. 6, line 11-p. 7, line 19, for example.

6. Grounds of Rejection to be Reviewed on Appeal

Claims 1-10 and 12-20 stand rejected under 35 U.S.C. § 102(e) based on Hauck.

7. Argument

A. Rejection under 35 U.S.C. § 102(e) over Hauck

The rejection under 35 U.S.C. § 102(e) does not follow MPEP § 706.02(V) which states at page 700-23 "for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly." In contrast with this clear requirement, the final Office Action bases an anticipation rejection on portions of Hauck, which do not teach each feature of the claimed combination of elements and thus cannot anticipate the presently claimed invention. For the above reason, this rejection should be reversed.

Claim 1

Claim 1 addresses a system for control of access to or distribution of data or software, comprising means for storing the software or data, and for storing a list of identifiers for licensed client nodes, as well a client application at each client node, performing authentication taking place at the client node by comparing the client identifier for the node against the list. Hauck addresses systems and techniques for managing access to web sites by remote users. A client side software program is used to generate a machine specific identifier, which is in turn used to authenticate a client machine to a server. A session identifier is established for an authenticated client, and the session identifier is maintained in a remote temporary storage table storing session identifiers for authorized machines. Each request for access from a client to a server includes the

session identifier and the temporary storage table is consulted to establish the authenticity of the submitted session identifier before responding to the request for access.

Claim 1, by contrast, addresses a system for control involving authentication taking place at the client node, in which the appearance of the client node's identifier on a list of identifiers of authorized clients is examined by a client application at the client node in order to determine whether the client node will allow access to software or data. Hauck does not teach and does not make obvious such authentication, but instead teaches examination by a server of a storage table for the appearance of a session identifier submitted by a client.

The Official Action relies on Hauck, col. 7, lines 23-32, which teaches a client side download linking library (DLL) which generates a specific client machine identifier and which includes an algorithm to insure that a password uniquely corresponding to the machine specific identifier is entered before access to protected data is granted. Hauck does not teach, however, that the client side application controls access to protected content, and does not teach that this client side application compares the client machine identifier against a list before allowing access to content.

In Hauck, at an initial request for protected content, a server supplies a client side DLL to the requesting client machine, and this DLL is used to generate a client machine identifier and also to require entry of a password corresponding to the client machine identifier before proceeding further in obtaining access to protected content. This process does not involve comparison of the client machine identifier against a list, and Hauck makes it clear that the server receives information from a client machine and compares the client machine information against a storage table in granting or denying requests for content. See Hauck, col. 8, line 13-col. 10, line 15. A user makes an initial request for protected content, which is accompanied by a

request for a password. A password appropriate to the client machine identifier is computed and transmitted appropriately. A user entering appropriate subscription information is given a corresponding password by a server and is prompted to enter the password by the client side application. Upon entry, the entered password is compared with the transmitted password and a failure results in denial of access to content.

However, this comparison does not involve comparison by a client application of a client machine identifier against a list, and a successful entry is what leads to the step of entering client machine information in a list against which comparisons are made. See in particular Hauck, col. 9, lines 15-27, in which a session identifier is generated and loaded to a temporary storage table. Subsequent requests for protected content during a session are accompanied by transmission of the session identifier to the server, and the server compares the session identifier against the temporary storage table.

The system of claim 1, on the other hand, manages control of content based on decisions made by the client based on the appearance of the client's identifier in a list. This procedure allows for a more localized control without a need to involve a server for control of access, and can be used to manage content of information that can be freely distributed, but only usable on authorized machines, such as distribution on a CD, where the CD is not usable on machines whose identifier does not appear on a list. Claim 1 therefore defines over the cited art and should be allowed.

Claims 9, 10, 13, and 16 all similarly address authentication of a device, such as a client node, data processing device serving as a client node, or self service terminal. An application executed on the device compares an identifier against a list of authorized identifiers, with the comparison taking place at the device. As noted above with respect to claim 1, such features are

not taught by Hauck. Claims 9, 10, 13, and 16 therefore define over the cited art on the same basis as does claim 1.

8. Conclusion

The rejection of claims 1-10 and 12-20 should be reversed and the application promptly allowed.

Respectfully submitted,

Peter H. Priest
Reg. No. 30,210
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, NC 27713
(919) 806-1600

CLAIMS APPENDIX

1. A system for a licensee to control access to or distribution of software and/or data among a plurality of client nodes, the system comprising:

means for storing software and/or data that is to be made available to predetermined licensed client nodes, each client node of the plurality of client nodes being a data processing device for which access to specified software or data may be allowed if licensed, and for storing a list of identifiers for licensed client nodes, each identifier uniquely identifying one of the predetermined nodes, the presence of each identifier on the list authorizing the predetermined client node associated with the identifier to be allowed access to the software and/or data; and

a client application at each client node, the client application performing authentication taking place at the client node, authentication being accomplished by comparing the client identifier for the node against the list and allowing or rejecting access to the software and/or data by the client node at which the client application resides based on evaluation by the client application at the client node as to whether the identifier of the client node appears in the list.

2. A system as claimed in claim 1, wherein the means for storing the software and/or data and the list of unique client identifiers is portable.

3. A system as claimed in claim 2, wherein the means for storing the software and/or data and the list of unique client identifiers comprises a compact disc.

4. A system as claimed in claim 2, wherein the means for storing the software and/or data and the list of unique client identifiers comprises a floppy disc.

5. A system as claimed in claim 1, wherein the client nodes are part of a communications network.

6. A system as claimed in claim 5, wherein the means for storing is provided in a shared information storage area of a server that can be remotely accessed by at least some or all of the client nodes.

7. A system as claimed in claim 1, wherein the client application is operable to generate a unique identifier for the client node on which the client application resides and compare this with the unique identifiers on the authorized list, thereby to identify whether the unique identifier for that node is on the list.

8. A system as claimed in claim 7, wherein the client executes a license management program which uses node specific data to generate the unique identifier.

9. A method for a licensee to control access to or distribution of software and/or data among a plurality of client nodes, the method comprising:

storing in association with the software and/or data, a list of unique identifiers for licensed client nodes, each of which uniquely identifies one of the nodes authorized to be allowed access to the software and/or data;

identifying at each node whether a unique identifier for a particular node is included on the list; and

controlling the operation of each node so that the list is examined at each node and the unique identifier is compared against the list, and loading, installation, or use of the software and/or data is allowed or rejected based on the comparison at the client node of the unique identifier against the list.

10. A program storage device, readable by a machine, having encoded thereon instructions executable by the machine for:

executing a license management program to establish a unique identifier associated with the machine executing the instructions;

reading a list of unique identifiers associated with specified software and/or data, each unique identifier being uniquely associated with one of a plurality of machines and establishing its associated machine as licensed for the specified software and/or data; and

controlling the operation of a client node comprising the machine executing the instructions so as to allow or reject access by the machine to the software and/or data based on a comparison taking place at the client node of the unique identifier for the client node against the list of unique identifiers.

11. (canceled)

12. A program storage device as claimed in claim 10, wherein the instructions encoded thereon include instructions for generating the unique identifier using node specific data.

13. A data processing device serving as a client node comprising:

means for reading a list of unique identifiers associated with software and/or data, each unique identifier being uniquely associated with one of a plurality of client nodes or terminals licensed to use the software and/or data; and

means for controlling the operation of the data processing device so that the data processing device examines its own unique identifier and the list of unique identifiers and allows or rejects loading, installation, or use of the software and/or data based on a comparison taking place at the data processing device of its own unique identifier against the list of unique identifiers.

14. A data processing device as claimed in claim 13, further comprising:

means for generating a unique identifier for the node implemented by the data processing device and comparing this with the unique identifiers on the authorized list, thereby to identify whether the unique identifier for that node is on the list and licensed.

15. A data processing device as claimed in claim 14, wherein node specific data is used to generate the unique identifier.

16. A self-service terminal comprising:

means for reading a list of unique identifiers associated with software and/or data, each unique identifier being uniquely associated with one of a plurality of self-service terminals licensed to use the associated software and/or data; and

means for controlling the operation of the self-service terminal so that the self-service terminal examines a unique identifier associated with the self-service terminal and the list of unique identifiers and allows or rejects loading, installation, or use of the software and/or data based on a comparison taking place at the self-service terminal of the unique identifier of the self-service terminal against the list of unique identifiers.

17. A self-service terminal as claimed in claim 16 further comprising:

means for generating a unique identifier for the self-service terminal and comparing this with the unique identifiers on the authorized list, thereby to identify whether the unique identifier for the self-service terminal appears on the list.

18. A self-service terminal as claimed in claim 17, wherein node specific data is used to generate the unique identifier.

19. The self-service terminal as claimed in claim 16, wherein the self-service terminal is an automated teller machine in a network comprising a plurality of automated teller machines operated by a common operator licensed to utilize the associated software and/or data.

20. The self-service terminal as claimed in claim 19, wherein the automated teller machine executes license management software to generate its associated identifier, and wherein said list of unique identifiers licensed to utilize the associated software and/or data is generated at a remote server which communicates with the automated teller machine over the network.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.